

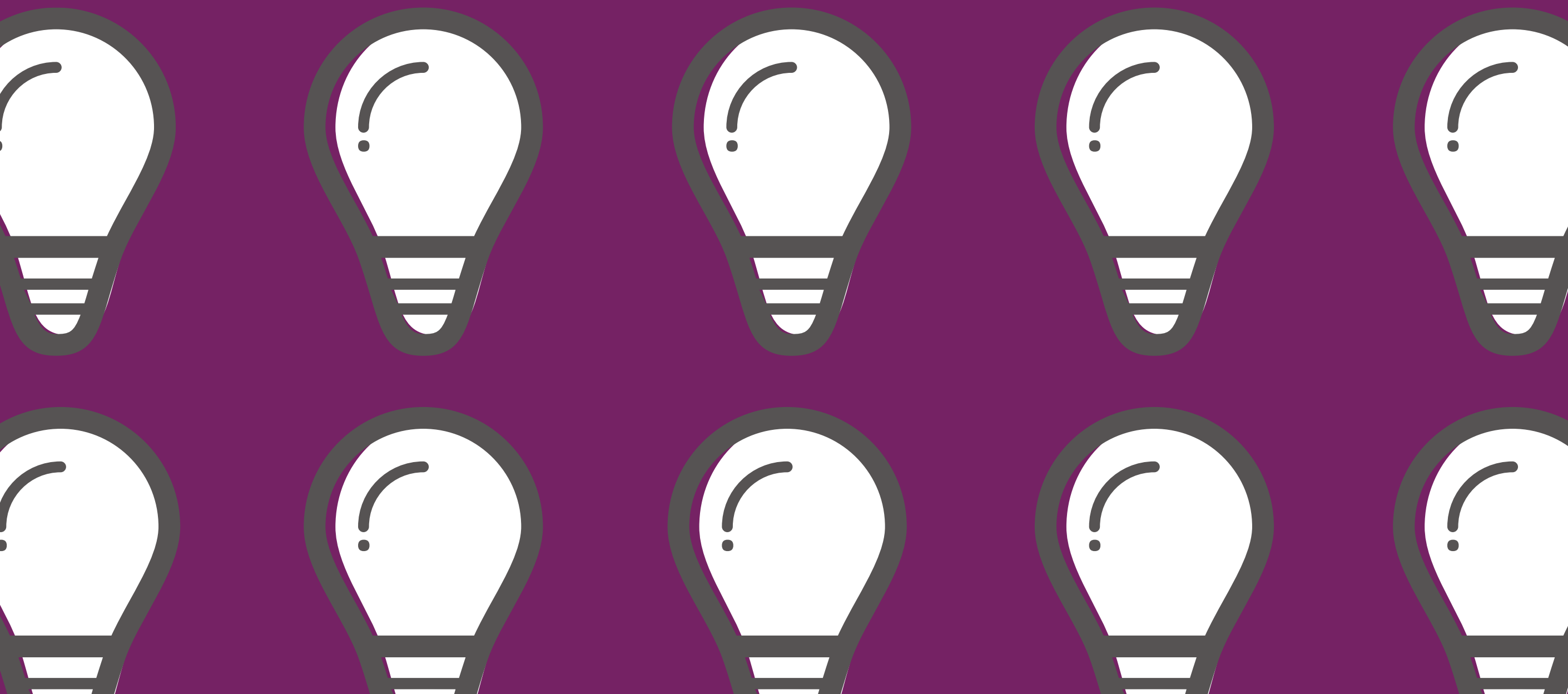
GIACOMO CASOLO

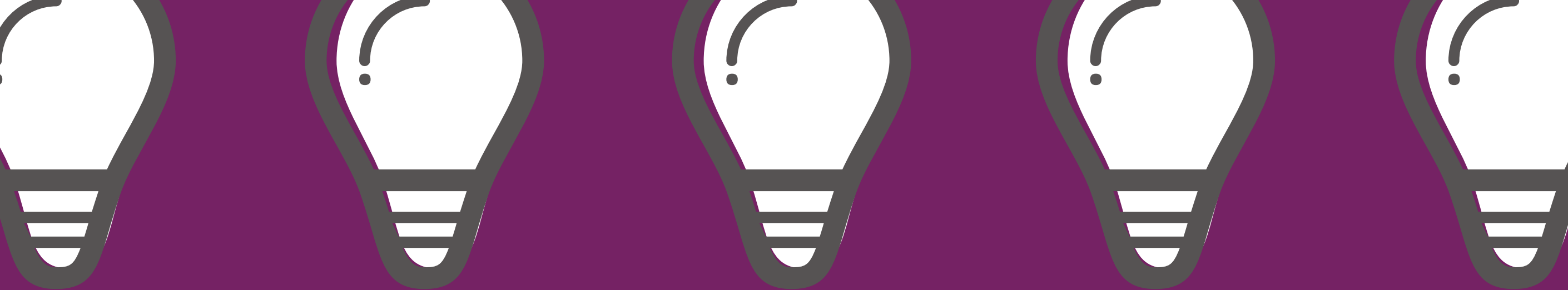
BITCOIN E BLOCKCHAIN

Manuale per la comprensione



BLOCKCHAIN





INDICE:

- PREMESSA
- OBIETTIVI
- CHI SONO
- STORIA DI BITCOIN
- TECNOLOGIA
BLOCKCHAIN
- BLOCKCHAIN 2.0
- CONCLUSIONI



PREMESSA

Ciao!

Se hai scaricato questo manuale, significa che hai deciso di rompere gli indugi e vuoi davvero capire che cosa sta succedendo là fuori.

Stiamo vivendo un momento davvero eccitante e di grande cambiamento.

I rumors intorno a Bitcoin e Blockchain sono ai massimi storici, tuttavia solo un ristretto numero di persone ha davvero compreso di cosa stiamo parlando e cosa sta accadendo. Questo da un lato può essere un bene, ma dall'altro anche un grande male: *in un momento di grande confusione e di scarsa informazione si possono commettere gravi errori. Il principale secondo me è scambiare la volatilità dell'attuale mercato delle cripto monete dovuto a*

speculazioni con la poca affidabilità di questa nuova tecnologia.

L'obiettivo di questo piccolo ebook è uno ed uno solo: **spiegare in modo semplice e chiaro**

che cos'è Bitcoin e Blockchain. Mi rendo conto che è una sfida ambiziosa e che nelle precedenti righe ho usato termini e introdotto concetti come volatilità, mercato e speculazioni che non sono probabilmente di immediata comprensione. Non ti preoccupare li chiariremo successivamente.

Il primo passo per comprendere il mondo delle cryptovalute e la tecnologia Blockchain è studiare e imparare le basi. Questo breve ebook parte proprio da Bitcoin, il nonno delle cryptovalute, e dalla tecnologia Blockchain nel suo

funzionamento basico. Queste informazioni ti permetteranno di comprendere come funzionano le cryptovalute e Blockchain 2.0 (argomento che tratterò nel seguito di questo ebook).

Sei pronto? Iniziamo!

OBIETTIVI

Prima di procedere ecco la mia promessa: una volta concluso questo ebook sarai in grado di rispondere a queste domande:

- Che cos'è Bitcoin?
- Qual'è la sua storia e chi l'ha creato?
- Che cos'è la tecnologia Blockchain?
- Chi sono i minatori?
- Quali sono le conseguenze sociali ed economiche di Bitcoin e Blockchain?
- Perché parliamo di rivoluzione?

CHI SONO

Giustamente ti starai chiedendo chi sono e perchè dovresti dedicare il tuo tempo alla lettura di questo manuale. Ecco quindi una breve introduzione sulla mia persona.

Mi chiamo Giacomo ho 26 anni e sono un giovane ed appassionato marketer.

Ho creato questo ebook per diffondere la conoscenza base della rivoluzione che sta avvenendo. Una rivoluzione che modificherà sostanzialmente il modo in cui vediamo ed utilizziamo la tecnologia e tutto quello che ad essa è connesso. Una rivoluzione che si chiama Blockchain.

Ritengo infatti che come è avvenuto un cambiamento epocale negli anni '90 con l'avvento di Internet, un altrettanto

significativo cambiamento è stato progettato, ha trovato nella contingenza socio-tecnologico-economica odierna terreno fertile ed il suo arrivo nelle disponibilità alle masse è solo questione di tempo. Un cambiamento di tale portata implica conseguenze a cascata su numerose dinamiche che oggi scandiscono la nostra quotidianità e questo si traduce in conseguenze sulla società, il mercato ed i suoi attori.

Il mio pensiero è che un nuovo paradigma sta conquistando il web e le sue estensioni offline.

Comprenderlo, immaginarlo ed intuirne le applicazioni il prima possibile se non doveroso è quantomeno necessario.

Il mio obiettivo è tradurre tutto questo in soluzioni e strategie di marketing adeguate per una rete che cambia.

STORIA DI BITCOIN

Bitcoin, il nonno delle criptomonete, nasce nel 2009 per opera di una persona (o gruppo di persone) sotto lo pseudonimo di **Satoshi Nakamoto**.

Per definire cos'è Bitcoin potremmo dire che si tratta della moneta di Internet.

Chiunque nel mondo può aprire un account ed accedere al servizio attivo 24/7. Gli unici strumenti che servono sono un computer e la connessione Internet. Il trasferimento dei fondi richiede solo pochi minuti anche se due persone si trovano agli estremi del mondo.

Per comprendere meglio l'importanza di ciò che ha segnato Bitcoin ed in particolare le proprietà di Blockchain, dobbiamo introdurre il concetto di **decentralizzazione**.

In riferimento a Bitcoin parliamo di decentralizzazione per intendere il fatto che **nessuna entità centrale governa il sistema**. Nessuna banca o stato controlla il network Bitcoin.

All'atto pratico dunque che cosa comporta la decentralizzazione? Innanzitutto significa che *nessuna entità potrà aggiungere 1 solo bitcoin all'interno del network (max 21MLN), prevenendo la possibilità di svalutarlo come invece accade per le valute FIAT (Euro, Dollaro, etc)*. In secondo luogo, ma lo capiremo meglio nel paragrafo dedicato a Blockchain, la decentralizzazione implica il fatto che *contemporaneamente su tutti i nodi della rete (computer collegati) sono accessibili ma criptati e imm modificabili i dati di ogni singola transazione*.

La decentralizzazione di Bitcoin è dovuta alla natura della sua struttura: **P2P, Peer-to-Peer è un modello di architettura logica di rete informatica dove i nodi (“computer collegati al network”) non sono gerarchizzati unicamente sotto forma di client o server fissi (clienti e serventi), ma sotto forma di nodi equivalenti o paritari (in inglese peer) che possono cioè fungere sia da client che da server verso gli altri nodi terminali (host) della rete.**

La non-necessità di fiducia in terze parti invece è una caratteristica che dipende dalla tecnologia Blockchain e la analizzeremo nel paragrafo successivo.

Un altro aspetto rilevante di Bitcoin, comune a tutte le altre cryptovalute, riguarda l'essere **open-source**.

Ciò significa che il codice di Bitcoin è accessibile a chiunque e quindi chiunque può contribuire ad implementarlo, risolvere eventuali problematiche o verificare la sua natura.

Basta visitare il seguente indirizzo web <https://github.com/bitcoin/bitcoin>

Potremmo anche dire che l'open-source è lo spirito delle cryptomonete, infatti in questo mondo la comunità ed il rispetto di essa è fondamentale.

Ultimo elemento importante di Bitcoin e in parte comune ad alcune altre crypto sono i **Minatori**. Cercherò di spiegare chi sono e cosa fanno senza entrare in ambito tecnico. Sono i custodi del network Bitcoin. *Minare significa risolvere difficilissimi problemi matematici mettendo a disposizione la potenza di calcolo del proprio computer.*

I minatori che risolvono questi problemi vengono ripagati in Bitcoin. A questo punto ti starai chiedendo perchè devono risolvere questi problemi..?

Quando una transazione viene effettuata sul network è immediatamente distribuita su tutti i nodi della rete che così vengono allertati. Per convalidare la transazione è necessario però che un minatore risolva il difficile problema matematico, ecco perchè esistono e perchè devono farlo. Altrimenti la transazione non sarebbe valida.

Con il boom che Bitcoin ha avuto sia in termini di diffusione che in termine di valore unitario, molti sono coloro che hanno deciso di fare i minatori. Tuttavia, con un interesse così alto, il lavoro del minatore è cresciuto moltissimo e la

potenza di calcolo necessaria per risolvere i problemi è aumentata esponenzialmente comportando un costo energetico elevatissimo. Sono quindi nate vere e proprie compagnie con ingenti capitali che hanno costruito data center enormi in paesi dove l'energia ha un costo più ridotto (come la Mongolia) per fare profitto attraverso il "mining".

Prima di passare a Blockchain, vorrei chiarire un piccolo gossip.

Probabilmente avrai spesso sentito collegare Bitcoin a crimini sul web... Spesso questo aspetto viene sollevato dai delatori. In realtà, come spesso accade, la storia è un pò diversa. Tutto va ricondotto a **Silk Road**, un portale anonimo del deep web dove era possibile acquistare tutto, ma proprio di tutto (droga, armi, documenti contraffatti).

In un posto del genere Bitcoin ha trovato applicazione come moneta. Ma è importante tenere a mente che non è nato per quello e un impiego errato di qualcosa non significa che quel qualcosa sia di per sé sbagliato. I soldi che oggi avete nel portafoglio e che avete onestamente guadagnato, sono gli stessi soldi con cui si comprano armi o droga e sono gli stessi soldi che arricchiscono i criminali. Quindi dobbiamo eliminare gli Euro? Non credo, a meno che non si passi totalmente alle crypto :)

La stessa domanda ce la si pone per Ross Ulbricht, il fondatore di Silk Road. Il 30 Maggio 2015 è stato condannato in primo grado all'ergastolo per i reati di associazione per delinquere, frode informatica, distribuzione di false identità, riciclaggio di denaro, traffico di droga, traffico di droga su internet e

conspirazione per trafficare droga. La questione è che Ross mica vendeva questi articoli o guadagnava dalla loro vendita..ha semplicemente creato uno spazio dove fosse possibile effettuare acquisti in anonimato e utilizzando una moneta alternativa, che poi sia stato usato per scopi criminosi non credo giustifichi imputargli l'atto criminale in sè condannandolo ad una pena senza fine.

Ma questa è un'altra storia.

BLOCKCHAIN TECHNOLOGY

Prima di dire di cosa si tratta vorrei chiederti di fare tuoi due concetti che ti aiuteranno nell'interpretare correttamente Blockchain.

1) Inizia a ragionare in termini di “scambio di valore”, dove valore è inteso nell’accezione più ampia: economico, informazione e dato sensibile.

2) Inizia a ricordarti che Internet è basato su scambi, scambi di valore: informazioni tra server e client, messaggi di posta elettronica, transazioni economiche, firme digitali, contenuti, privacy.

Leggi ora la mia interpretazione del significato di Blockchain:

scambiare valore in modo sicuro, decentralizzato, immutabile ed incorruttibile nel tempo, anonimo.

Prima ancora di scendere nel dettaglio penso che potrai aver intuito perchè BC è una rivoluzione: dato per assodato cosa intendiamo per scambio di valore e compreso che il web si basa su questo, allora – leggendo la definizione di BC – capirai come essa ottimizzi tale scambio a dei livelli mai raggiunti prima (sicuro, decentralizzato, immutabile ed incorruttibile, anonimo).

Ora credo tu sia pronto per leggere la definizione tecnica di blockchain:

“La blockchain (in italiano letteralmente: catena di blocchi) è una lista in continua crescita di record, chiamati blocks, che sono collegati tra loro e resi sicuri mediante l’uso della crittografia.

Ogni blocco della catena contiene un Puntatore hash come collegamento al blocco precedente, un timestamp e i dati della transazione.

Blockchain, è fondamentalmente un registro aperto e distribuito che può registrare le transazioni tra due parti in modo efficiente, verificabile e permanente. Per questo utilizzo, questo database sfrutta una rete Peer-to-peer che si collega ad un protocollo per la convalida dei nuovi blocks.

Una volta registrati, i dati in un blocco non possono essere retroattivamente alterati senza che non vengano modificati tutti i blocchi successivi ad esso, il che necessiterebbe di una collusione della maggioranza della rete”.

Chiariti i presupposti, vorrei approfondire l'aspetto più filosofico della questione, l'aspetto per cui si è generato tutto questo incredibile fervore e indotto che troppo spesso in modo errato viene ricondotto solo all'ormai noto Bitcoin.

L'aspetto cruciale è la decentralizzazione, sicurezza e inalterabilità che porta Blockchain.

Riprendiamo per un secondo la definizione che menziona la parola "registro". Possiamo dunque intendere blockchain come un libro mastro contenente questi "scambi di valore" di cui ti ho parlato in precedenza.

La rivoluzione principale avviene proprio a questo livello: *tipicamente un libro mastro analogico o digitale che fosse era nelle mani di un'autorità centrale che si occupava di redigerlo/aggiornarlo, un'autorità in cui si doveva riporre fiducia, un'autorità che garantiva correttezza e sicurezza solo in base al fatto di essere l'autorità.*

Con la decentralizzazione invece l'autorità viene distribuita a tutti i partecipanti del libro mastro.

Infatti questo libro mastro non è più nelle disponibilità di un unico attore ma è condiviso sempre con tutta la rete che partecipa. Dunque *le informazioni contenute sono sempre visibili da tutti ma immutabili e inalterabili proprio grazie alla natura e struttura di Blockchain.*

Senza ancora scendere nel dettaglio, credo tu possa comprendere la potenza di questo nuovo passo: ***poter garantire che qualcosa di estremamente importante non possa essere modificato/alterato dal volere del singolo che ne dispone e permetterne l'accessibilità a tutti in ogni momento, mette tranquillità solo a pensarlo!***

A questo punto dovresti anche intuire come tutto questo sia trasferibile non solo all'ambito finanziario (maggiore sicurezza nelle transazioni, moneta che

non risente di logiche di potere e di politica, abbattimento dei costi di transazione), ma anche nell'ambito politico, sociale e aziendale. Ecco che arriviamo a Blockchain 2.0 ed ai progetti post Bitcoin.

BLOCKCHAIN 2.0

Questo paragrafo ha l'obiettivo di spiegarti come all'atto pratico questa nuova tecnologia può applicarsi al nostro quotidiano e quale valore porterebbe cambiando sostanzialmente le regole del gioco.

Se infatti fosse possibile esprimere una votazione politica, la partecipazione ad un progetto sociale, la possibilità di certificare per l'utente un'origine controllata di un prodotto all'interno di una filiera, la possibilità di gestire rapporti interni aziendali e tra diverse

aziende secondo i criteri di decentralizzazione, sicurezza ed inalterabilità cosa succederebbe?

Significherebbe che tutte le applicazioni che oggi siamo intenti ad utilizzare per professione, svago o servizi, non avrebbero più bisogno di un'entità centrale, di un intermediario, di quelli che vengono definiti Middlemen.

Decadrebbe la necessità di avere grandi compagnie (penso a Facebook, Uber, AirBnb, Amazon) che detengono dati e informazioni sui loro server centralizzati, perchè esse sarebbero presenti e accessibili sempre su tutti i nodi della rete ovvero nella disponibilità della comunità che ne partecipa. Un sensibilissimo risparmio di costi di intermediazione e una

sicurezza/proprietà effettiva sui dati mai raggiunta prima.

Gli esempi sopra riportati introducono Blockchain 2.0 e menzionano gli smart contract.

Con il termine Blockchain 2.0 si intende la fase post Bitcoin che ha visto la nascita di progetti su tecnologia blockchain legati a piattaforme per applicazioni decentralizzate. Parliamo di Ethereum, Lisk ed Eos ad esempio.

Con questi progetti, come anticipato, entrano in gioco gli smart contract.

Tecnicamente essi non sono una scoperta recente. Di smart contract già si parlava nei primi '90. Come esempio potremmo indicare le licenze dei software: lo smart contract “sa” che, nel momento in cui si verifica la condizione per cui l'abbonamento è pagato,

il software deve essere utilizzabile. Alla scadenza ne viene impedito l'accesso. Molto semplice.

Blockchain ha permesso di supportare in maniera più efficiente gli smart contract. Essi dunque permettono di automatizzare dei rapporti contrattualizzati. La tecnologia verifica infatti che condizioni e clausole contenute nel contratto si siano realizzate ed esegue automaticamente il contratto stesso in modo decentralizzato, sicuro ed incorruttibile. La difficoltà di oggi è appunto riuscire a condensare in regole precise e chiare le condizioni e le clausole dei contratti per poterne permettere questo tipo di esecuzione.

Con Blockchain 2.0 quindi si passa dal mero strumento finanziario/di

pagamento come Bitcoin a progetti che, mantenendo i valori di decentralizzazione, sicurezza ed inalterabilità, migliorano processi umani riducendo costi e tempo ed innalzando gli standard di controllo.

CONCLUSIONI

Bene! Siamo arrivati alla conclusione di questo breve ebook. Spero che ora tu possa avere maggiore consapevolezza di ciò che Bitcoin e Blockchain sono e che tu voglia supportare il diffondersi di questa tecnologia.

Come avrai capito io ne sono un fiero sostenitore ed anche non sapendo di cosa ti occupi, sono convinto che anche il tuo settore verrà totalmente ripensato da questa tecnologia.

Grazie per l'attenzione che hai dedicato a questa lettura. Se volessi approfondire ulteriormente questi argomenti, non esitare a contattarmi.

A presto,
Giacomo

CONTATTI

giacomocasolo.it

info@giacomocasolo.it

facebook.com/gcasolo

steemit.com/@giacomocasolo

Giacomo Casolo
GROWTH MRKT | BLOCKCHAIN